SYSTEM ACCESS CONTROL PROCEDURES

The System Managers/Owners must ensure that appropriate technical safeguards are implemented that allow access only to authorized users with a "need to know".

1. Granting and Revoking Access

For granting and revoking access, refer to LACDMH Policy No. 550.02, Workforce Members Security Policy.

2. Unique User Identification

Purpose: To uniquely identify and track each user or workforce member for the purpose of monitoring access control to all RO-managed networks, systems, and applications that contain EPHI

A. Any user or workforce member that requires access to any network, system, or application that access, transmits, receives, or stores EPHI, must be provided with a unique user identification string.

   a. System Managers/Owners must clearly define the naming/numbering format for system users.

   b. The system must be able to identify the unique user name and allow audit capabilities in accordance with the recommended safeguards specified in LACDMH Policy No. 558.01, System Audit Controls.

B. Systems connected/connecting to the County network must have a system login banner with the following language:

NETWORK DEVICES

This computer system (including all related equipment, network and Network devices) is the property of the County of Los Angeles and is provided for authorized use only. There is no expectation of privacy in this system.

Any or all uses or access of this computer system, including all of its data, may be monitored, interrupted, recorded, read, copied, or captured and disclosed in any manner for any lawful or authorized purpose, including disciplinary or civil action and criminal prosecution. Use or access of this system, authorized or unauthorized, constitutes consent to such monitoring, interception, recording, reading, copying or capturing and disclosure.

Unauthorized or improper use or access of this computer system may result in criminal, civil and/or administrative action. By continuing to use or access this system, you agree to these terms.

REMOTE LOGIN

You are about to access a computer system (including all related equipment, network and Network devices) which is the property of the County of Los Angeles and is provided for authorized use only. There is no expectation of privacy in this system.

Any or all uses or access of this computer system, including all of its data, may be monitored, interrupted, recorded, read, copied or captured and disclosed in any manner for any lawful or authorized purpose, including disciplinary or civil action and criminal prosecution. Use or access of this system, authorized or unauthorized, constitutes consent to such monitoring, interception, recording, reading, copying or capturing and disclosure.

Unauthorized or improper use or access of this computer system may result in criminal, civil and/or administrative action. By continuing to use or access this system, you agree to these terms.

C. Workforce member's passwords must follow requirements specified in LACDMH Policy No. 551.03, Workstation Use and Security Policy.

D. Each user and workforce member must ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications. If a user or workforce members believes their user identification has been comprised, it must be immediately reported in accordance with LACDMH Policy No. 552.01, Security Incident Report and Response Policy.

3. System Login Monitoring

System Managers/Owners must enable access logging by users or processes. Detailed specifications can be found in LACDMH Policy No. 558.01, System Audit Controls

4. Emergency access procedure

Refer to LACDMH Policy No. 550.03, Information Technology Contingency Plan Policy.

5. Automatic Logoff

LACDMH must implement password-protected screensaver on all systems that automatically prevents unauthorized users from viewing or accessing electronic protected health information or other sensitive data. Details for screen saver specifications can be found in LACDMH Policy No. 551.03, Workstation Use and Security Policy.

6. Encryption/Decryption

A. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

B. Confidential data (e.g., patient information) must be password protected, encrypted, or stored on a secure network drive.

C. Confidential data having a Sensitivity Score of "High" must be encrypted. For further details on encryption, refer to LACDMH Policy No. 551.03, Workstation Use and Security Policy.

7. Information System Access Control Review and Documentation

After performing a risk analysis and determining the Risk Analysis Sensitivity Score, System Managers/Owners must design access controls commensurate with the rating. For procedures on how to determine the Risk Analysis Sensitivity Score, refer to Attachment 1, Information Access Management Procedures, in LACDMH Policy No. 550.01, Security Management Process: LACDMH Risk Management.

The DISO, taking into consideration each system's Risk Analysis Sensitivity Score, must evaluate and approve the design, effectiveness, and implementation of the access controls to limit unauthorized access of Workforce Members to information systems, including workstations, servers, networks, and applications.

8. System Security Documentation

Electronic data systems that need access controls must have System Security Documentation that documents in detail the implementation of the access safeguards.